DETAILED ACTION

This Office Action is in response to Applicant's communication/amendment filed on 8/20/09 and a telephonic communication on Barry S. Goldsmith on 12/2/09.

Examiner Amendment

An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

The following changes were authorized by Barry S. Goldsmith in a telephone interview on 12/2/09.

Please replace claims 1, 7, 21, 26, 30 and 31 with the claims listed below:

--

1. (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including a database for storing a security policy including a plurality of rules that control user access to applications; and a policy distributor, coupled to the database, for distributing the plurality of rules through the network, wherein the policy manager comprises a processor;

(2) a security engine located on a client coupled to the network and stored on a computer readable storage medium, said security engine storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy

includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

(3) the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, each separate application in the system being guarded by a different access authorization service such that separate applications do not share authorization services; and wherein the security policy is updated by recording a series of incremental changes to the security policy, determining which of said incremental changes are applicable to said security engine, computing an accumulated delta that reflects the series of incremental changes applicable to said security engine and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the accumulated delta to update the local customized security policy,

wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the policy manager and sending the accumulated reversing delta to the security engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

7. (Currently Amended) A system for maintaining security for an application in a distributed computing environment, comprising:

an engine located at a client coupled to a network and stored on a computer readable storage medium, the engine storing a set of rules constituting a local customized policy received through the network from a centralized location, and enforcing the local customized policy at an application level of the client, wherein the centralized location comprises a processor;

an interface coupled to the engine for evaluating the local customized policy in order to control access to an application at the client wherein evaluating the local customized policy includes matching an access request to one or more of the plurality of

rules of the local customized policy and granting or denying access to the application based on the evaluation; and

the application, coupled to the interface so as to communicate with the engine, wherein the engine guards access to the application that is coupled to said interface each separate application in the system being guarded by a different access authorization service such that separate applications do not share authorization services;

wherein the local customized policy is updated by keeping track of incremental changes to the policy, determining which of said incremental changes are applicable to said engine, computing an accumulated delta that reflects all the incremental changes applicable to said engine and sending the accumulated delta to the engine from the centralized location such that the engine uses the delta to update the local customized policy,

wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the centralized location and sending the accumulated reversing delta to the engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

21. (Currently Amended) A computer implemented method for maintaining security in a distributed computing environment, comprising:

maintaining a policy manager coupled to a network, including a database for storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network, wherein the policy manager comprises a processor;

maintaining a security engine located on a client coupled to the network, storing a local customized security policy received through the network from the policy distributor, and enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of

the local customized security policy and granting or denying access to the application based on the evaluation; and maintaining the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, each separate application in the system being guarded by a different access authorization service such that separate applications do not share authorization services; and

receiving a series of incremental changes to the security policy at the policy manager;

determining which of said series of incremental changes are applicable to said security engine;

computing an accumulated delta that reflects the series of incremental changes that are applicable to said security engine; and

distributing the accumulated delta to the security engine on the client wherein the security engine uses the delta to update the local customized security policy, wherein each incremental changes to a security policy includes one or more rule changes in a security policy, and wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the policy manager and sending the accumulated reversing delta to the security engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

26. (Currently Amended) A computer implemented method for maintaining security in a distributed computing environment, comprising:

maintaining an engine at a client coupled to a network, the engine to store a set of rules constituting a local customized policy received through the network from a centralized location, and enforce the local customized policy at an application level of the client, wherein the centralized location comprises a processor;

maintaining an interface coupled to the engine for evaluating the local customized policy in order to control access to securable components wherein

evaluating the local customized policy includes matching an access request to one or more of the set of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintaining the application, coupled to the interface so as to communicate with the engine, wherein the engine guards access to the application that is coupled to said interface each separate application being guarded by a different access authorization service such that separate applications do not share authorization services;

receiving a series of incremental changes to the set of rules at the centralized location;

determining which of said incremental changes are applicable to said engine;

computing an accumulated delta to reflect the series of incremental changes that are applicable to said engine; and

communicating the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy,

wherein each incremental change to a policy includes one or more rule changes in a policy, and wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the centralized location and sending the accumulated reversing delta to the engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

30. (Currently Amended) A non-transitory computer readable storage medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain a policy manager coupled to a network, including a database storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network, wherein the policy manager comprises a processor;

maintain a security engine located on a client coupled to the network, for storing a local customized security policy received through the network from the policy

distributor, and enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintain the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, each separate application being guarded by a different access authorization service such that separate applications do not share authorization services; and receive a series of incremental changes to the security policy at the policy manager;

determine which of said series of incremental changes are applicable to said security engine;

compute an accumulated delta that reflects the series of incremental changes applicable to said security engine; and

distribute the accumulated delta to the security engine on the client wherein the security engine uses the delta to update the local customized security policy,

wherein each incremental changes to a security policy includes one or more rule changes in a security policy, and wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the policy manager and sending the accumulated reversing delta to the security engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

31. (Currently Amended) A non-transitory computer readable storage medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain an engine at a client coupled to a network, the engine to store a set of rules constituting a local customized policy received through the network from a centralized location, and enforce the local customized policy at an application level of the client, wherein the centralized location comprises a processor;

maintain an interface coupled to the engine evaluating the local customized policy in order to control access to securable components wherein evaluating the local customized policy includes matching an access request to one or more of the set of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and

maintain the application, coupled to the interface so as to communicate with the engine,

wherein the engine guards access to the application that is coupled to said interface each separate application being guarded by a different access authorization service such that separate applications do not share authorization services;

receive a series of incremental changes to the set of rules at the centralized location;

determine which of said series of incremental changes are applicable to said engine;

compute an accumulated delta to reflect the series of incremental changes applicable to said engine; and

communicate the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy,

wherein each incremental changes to a policy includes one or more rule changes in a policy, and wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta and sending the accumulated reversing delta from the centralized location to the engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order.

--

Examiner's Statement of Reasons for Allowance

In light of applicant's arguments/amendments and the examiner amendment authorized by applicant's representative claims 1-9 are 21-31 are allowed.

Although Brownlie et al. (USPN 6202157) teaches distributing policy from a policy distributor to local client security policy engines enforcing the policies locally and newly discovered art Morris (USPN 5634052) teaches restoring baked up file versions using accumulated delta, neither those reference (alone or in combination) nor any other encountered prior art teach using accumulated delta as specified by the claim language to distribute policies locally enforcing access to application or, using the claim language, a policy distributor distributing the plurality of rules through the network and a security engine located on a client coupled to the network and stored on a computer readable storage medium, said security engine storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and enforcing the local customized security policy with respect to an application at the client wherein enforcing the local customized security policy includes evaluating an access request by matching it to one or more of the plurality of rules of the local customized security policy and granting or denying access to the application based on the evaluation; and the application, coupled to the security engine, wherein the security engine guards access to the particular application to which said security engine is coupled, each separate application in the system being guarded by a different access authorization service such that separate applications do not share authorization services; and wherein the security policy is updated by recording a series of incremental changes to the security policy, determining which of said incremental changes are applicable to said security engine, computing an accumulated delta that reflects the series of incremental changes applicable to said security engine and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the accumulated delta to update the local customized security policy, wherein a previously enforced version of the local customized security policy is reconstructed by generating an accumulated reversing delta at the policy manager and

sending the accumulated reversing delta to the security engine, wherein the accumulated reversing delta comprises a sequence of incremental changes in a reverse order, as required by the independent claim 1 (and the similarly drafted independent claims), for example.

The prior art, fails to anticipate or fairly suggest the limitation of applicant's independent claims, in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. As a result the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on statement of Reasons for Allowance".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the Group receptionist whose telephone number is (571) 272-1600.

/Peter Poltorak/

Examiner, Art Unit 2434

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434